AD-A065 363 NAVAL WEAPONS CENTER CHINA LAKE CALIF F/G 9/3
PROPOSED COMPLEX AND BINARY SEQUENCES WHICH ACHIEVE WELCH BOUND--ETC(U)
JUN 76 W O ALLTOP, F G FREYNE

UNCLASSIFIED NWC-TM-2790 GIDEP-E095-1520 NL

1 OF 1
ADA
065363

END
DATE FILMED
4-79
DDC

LEVEL

NWC Technical Memorandum 2790

(6) PROPOSED COMPLEX AND BINARY SEQUENCES WHICH ACHIEVE WELCH BOUND.

by

(10) W.O. Alltop
Systems Development Department

and

F.G. Freyne
Fuze Department

NAVAL WEAPONS CENTER
China Lake, California 93555

8 MAY 1978

GOVERNMENT–INDUSTRY DATA EXCHANGE PROGRAM

GENERAL DOCUMENT SUMMARY SHEET

1 OF 1

Please Type All Information – See Instructions on Reverse

1. ACCESS NUMBER	2. COMPONENT/PART NAME PER GIDEP SUBJECT THESAURUS
E095-1520	General Technical Data, Test & Reliability Mathematics
3. APPLICATION	**4. MFR NOTIFICATION** / **5. DOCUMENT ISSUE (Month/Year)**
Engineering	☐ NOTIFIED ☒ NOT APPLICABLE / June 1976
6. ORIGINATOR'S DOCUMENT TITLE	**7. DOCUMENT TYPE**
Proposed Complex & Binary Sequences which Achieve Welch Bound	☒ GEN RPT ☐ NONSTD PART ☐ SPEC
8. ORIGINATOR'S DOCUMENT NUMBER	**9. ORIGINATOR'S PART NAME/IDENTIFICATION**
NWC TM 2790	N/A
10. DOCUMENT (SUPERSEDES) (SUPPLEMENTS) ACCESS NO.	**11. ENVIRONMENTAL EXPOSURE CODES**
None	N/A
12. MANUFACTURER	**13. MANUFACTURER PART NUMBER** / **14. INDUSTRY/GOVERNMENT STANDARD NUMBER**
N/A	N/A / N/A

15. OUTLINE, TABLE OF CONTENTS, SUMMARY, OR EQUIVALENT DESCRIPTION

Families of periodic sequences with small side-lobes and low cross-talk (cross-correlations) are needed in many digital communication systems. L. R. Welch has recently established a lower bound for the largest of the side-lobes and cross-correlation coefficients associated with a family of M distinct sequences of period L. In particular, for two sequences there must occur a coefficient greater than $(2L)^{-\frac{1}{2}}$. As the number M of sequences increases to approximately L^2, this lower bound increases to $L^{-\frac{1}{2}}$. In this report several sets of periodic sequences utilizing complex, ternary, and binary coded signal bits are constructed which nearly meet Welch's bound for M approximately equal to L^2. In this paper's context, ternary coding refers to three distinct phase signals, while complex coding refers to phase levels relating to the n^{th} complex roots of unity. Most of these sequences contain only L^2 non-zero entries. However, one type of family consists of $M = 2^m$ binary (± 1) sequences of period $L = 2^m - 1$. The maximum coefficient for this family is approximately one-half as large as the corresponding maximum for the Gold sequences of the same period. This represents a considerable improvement over the Gold codes for such codes requiring an even number of shift register stages for generation.

+ or -

2 to the m power

Sq. rt. L

Sq. rt. (1/L)

Sq. rt. (1/2L)

78 11 28 127

16. KEY WORDS FOR INDEXING	Coding Technique; Binary Sequences; Correlation Coefficients; Ternary Sequences (Doc Des--P)
17. GIDEP REPRESENTATIVE	**18. PARTICIPANT ACTIVITY AND CODE**
M. H. Sloan	Naval Weapons Center, China Lake, (X7)

DD FORM 1 OCT 77 2000

16

FOREWORD

The research described in this report was carried out from July 1975 through May 1976 under the authorization of Task Area Number ZR000-01-01. This represents part of a continuing investigation of coding techniques being performed in conjunction with and partially funded by the Fuze Exploratory Development Program, Task Area Number F32-352-501.

This report is released at the working level. Because of the continuing nature of the coding research project, these results are subject to refinements and modifications.

Reviewed by
H. A. BULGERIN
Head, Advanced Systems Division
Fuze Department

Released by
LEE E. LAKIN, JR.
Head, Computer Sciences Division
Systems Development Department
18 June 1976

CONTENTS

4

ABSTRACT

Families of periodic sequences with small side-lobes and low cross-talk (cross-correlations) are needed in many digital communication systems. L. R. Welch has recently established a lower bound for the largest of the side-lobes and cross-correlation coefficients associated with a family of M distinct sequences of period L. In particular, for two sequences there must occur a coefficient greater than $(2L)^{-\frac{1}{2}}$. As the number M of sequences increases to approximately $L^{\frac{1}{2}}$, this lower bound increases to $L^{-\frac{1}{2}}$. In this report several sets of periodic sequences utilizing complex, ternary, and binary coded signal bits are constructed which nearly meet Welch's bound for M approximately equal to $L^{\frac{1}{2}}$. In this paper's context, ternary coding refers to three distinct phase signals, while complex coding refers to phase levels relating to the n^{th} complex roots of unity. Most of these sequences contain only $L^{\frac{1}{2}}$ non-zero entries. However, one type of family consists of $M = 2^m$ binary (±1) sequences of period $L = 2^m - 1$. The maximum coefficient for this family is approximately one-half as large as the corresponding maximum for the Gold sequences of the same period. This represents a considerable improvement over the Gold codes for such codes requiring an even number of shift register stages for generation.

5

1. INTRODUCTION

The need for sets of sequences possessing low periodic cross correlations and auto-correlation side-lobes frequently arises in communications problems. A recent paper of Welch[1] presents a lower bound for the maximum absolute value of these correlation coefficients as a function of the period L and the number M of sequences in the set. The Gold sequences,[2] which have period $L = 2^m - 1$, differ from the bound W(L,M) of Welch by factors of approximately 2 and $2^{\frac{1}{2}}$ for m even and m odd, respectively. Here we describe sets which achieve the bound W(L,M) as well as sets which approach it as L increases.

The sets presented in Sections 2 and 3 are formed by combining partial difference sets in cyclic groups with Fourier or Hadamard matrices. A partial difference set is a slight generalization of a planar difference set, which gives rise to a finite cyclic projective plane.[3,4] The planar difference sets are used to construct optimal and near-optimal sets of sequences. Additional near-optimal sequences are formed using certain of the relative difference sets of Elliott and Butson.[5] With only one exception the optimal sequences have complex entries. For each of these sets, L is approximately equal to K^2, and M equals K or K + 1, where

---

[1] L. R. Welch. "Lower Bounds on the Maximum Cross Correlation of Signals," *IEEE Trans. Inform. Theor.*, May 1974, pp. 397-399.

[2] R. Gold. "Optimal Binary Sequences for Spread Spectrum Multiplexing," *IEEE Trans. Inform. Theor.*, October 1967, pp. 619-621.

[3] L. D. Baumert. *Cyclic Difference Sets*. Berlin, Heidelberg, New York, Springer-Verlag, 1971.

[4] M. Hall, Jr. *Combinatorial Theory*. Waltham, Mass., Blaisdell, 1967.

[5] J. H. E. Elliott and A. T. Butson. "Relative Difference Sets," *Ill. J. Math.*, Vol. 10 (1966), pp. 517-531.

K is the number of elements in the underlying partial difference set, and L is the order of the cyclic group. The largest correlation coefficient has magnitude 1/K, and each sequence has exactly K non-zero entries.

The sequences described in Section 4 are derived from binary, cyclic error-correcting codes in much the same way as are the Gold sequences. For $L = 2^{2m} - 1$, a certain cyclic error-correcting code of length L and dimension 3m yields a near-optimal set of 2^m binary sequences. Like the Gold sequences, these have no zero entries and are easily generated by shift-register techniques. Their correlation bounds are easily obtained from the code weight distributions given by Kasami, Lin, and Peterson.[6]

2. DEFINITIONS AND NOTATION

We are interested in sets $A = \{a^1, a^2, \ldots, a^M\}$ of sequences of period L. Each a^ν is a complex L-vector $(a_0^\nu, \ldots, a_{L-1}^\nu)$ of norm 1; that is, $a_0^\nu \bar{a}_0^\nu + \ldots + a_{L-1}^\nu \bar{a}_{L-1}^\nu = 1$, where $\bar{a}$ denotes the complex conjugate of a. The correlation coefficients are given by

$$c_{\nu\lambda}(\tau) = \sum_{i=0}^{L-1} a_i^\nu \bar{a}_{i+\tau}^\lambda .$$

with subscripts reduced modulo L, $1 \leq \nu, \lambda \leq M$, $0 \leq \tau \leq L-1$. A measure of the correlation quality of the set A is $c_{max}(A)$, the maximum over all $|c_{\nu\lambda}(\tau)|$ with $\nu \neq \lambda$ or $\tau \neq 0$; i.e., the maximum over all of the auto- and cross-correlation coefficients except the "peaks" $c_{\nu\nu}(0) = 1$. A principal result from Welch[1] is that for any such family A, $c_{max}(A) \geq W(L,M)$, where

---

[6] T. Kasami, S. Lin, and W. W. Peterson. "Some Results on Cyclic Codes Which Are Invariant Under the Affine Group and Their Applications," *Inform. and Contr.*, Vol. 11 (1968), pp. 475-496.

7

$$W(L,M) = \left(\frac{M-1}{ML-1}\right)^{\frac{1}{2}}.$$

We define an (L,K) partial difference set to be a set $\Delta = \{d_1, \ldots, d_K\}$ of K distinct elements from the cyclic additive group Z_L of integers modulo L, such that for every non-zero x in Z_L there is at most one pair d_r, d_s from Δ satisfying $d_r - d_s = x$. From this condition one can easily show that L must be greater than $K^2 - K$. Associated with the partial difference set Δ is the binary sequence $z(\Delta) = (z_0, \ldots, z_{L-1})$ defined by

$$z_i = \left.\begin{array}{ll} 1 & \text{if } i \in \Delta \\ 0 & \text{if } i \notin \Delta \end{array}\right\}.$$

The requirement that $d_r - d_s = x$ for at most one pair from Δ is equivalent to forcing the x^{th} auto-correlation coefficient of $z(\Delta)$ to be 0 or 1, for all $x \neq 0$. If all the side-lobes are, in fact, equal to 1, then Δ is a planar difference set. In this case the family of translates $\Delta + t$, $t \in Z_L$, form the L lines of a cyclic projective plane of order K - 1, (see Baumert[3] and Hall[4]). (A planar difference set is a special case of a cyclic difference set.[3] For the general cyclic difference set Δ, the side-lobes for the associated sequence $z(\Delta)$ must be constant, but may be greater than 1).

Suppose Δ is an (L,K) partial difference set and $E = (e_{\nu i})$ is an M X K complex matrix with each row of norm 1. We define a set $A(\Delta;E)$ of M sequences of period L as follows. Each sequence a^ν is zero except for the entries corresponding to elements of Δ. The K non-zero entries in a^ν are determined by the ν^{th} row of E. More precisely

$$a_i^\nu = \left.\begin{array}{ll} e_{\nu r} & \text{if } i = d_r \in \Delta \\ 0 & \text{if } i \notin \Delta \end{array}\right\}.$$

8

Thus, a^{ν} is formed by replacing the 1's in $z(\Delta)$ with the entries from the corresponding row of E. Equivalently, one may consider the matrix E to be augmented by inserting zero-columns where zeros occur in $z(\Delta)$. The rows of the resulting $M \times L$ matrix are the sequences a^{ν}. The correlation coefficients for the set $A(\Delta;E)$ are easily obtained from the entries in E and $E\bar{E}^T$. For $\tau \neq 0$, $c_{\nu\lambda}(\tau) = e_{\nu i}\, e_{\lambda j}$ if $i = d_r$ and $j = i + \tau = d_s$, while $c_{\nu\lambda}(\tau) = 0$ if τ does not occur as a difference $d_r - d_s$. For $\nu \neq \lambda$, one obtains

$$c_{\nu\lambda}(0) = \sum_{i=0}^{L-1} a_i^{\nu}\, \bar{a}_i^{\lambda}$$

$$= \sum_{r=1}^{K} e_{\nu r}\, \bar{e}_{\lambda r}\ ,$$

which is the $\nu\lambda^{th}$ entry in $E\bar{E}^T$.

For n a positive integer let F_n denote the Fourier matrix with νi^{th} entry equal to $\omega^{(\nu-1)(i-1)}$, $1 \leq \nu,\ i \leq n$, where ω is a primitive n^{th} root of 1. H_n will denote an $n \times n$ Hadamard matrix of +1's and -1's, having only +1's in the first column. We let F_n° and H_n° be the $n \times (n-1)$ matrices resulting from deleting the first column from F_n and H_n, respectively. From the fact that $F_n\bar{F}_n = H_nH_n^T = nI_n$, it follows that $F_n(\bar{F}_n^{\circ})^T = H_n^{\circ}(H_n^{\circ})^T = nI_n - J_n$, where I_n and J_n are the $n \times n$ identity matrix and the $n \times n$ matrix of +1's, respectively.

3. THE TERNARY AND COMPLEX SEQUENCES

For each of our sets $A = A(\Delta;E)$, Δ will be one of two algebraically distinct types of (L,K) partial difference sets, and E will be $\alpha_K F^{\circ}_{K+1}$, $\alpha_K H^{\circ}_{K+1}$, or $\alpha_K H_K$, where $\alpha_K = K^{-\frac{1}{2}}$. The scalar α_K normalizes the rows of the resulting E's. In each case every entry of E has magnitude $K^{-\frac{1}{2}}$.

Thus, the correlation coefficients for $\tau \neq 0$ all have magnitude $1/K$ or 0. Every off-diagonal entry of $E\bar{E}^T$ is 0 for $E = \alpha_K H_K$, and $-1/K$ for $E = \alpha_K F^\circ_{K+1}$ or $\alpha_K H^\circ_{K+1}$. Therefore, $|c_{\nu\lambda}(0)| \leq 1/K$ for $\nu \neq \lambda$. Whenever E is one of these three matrices, we have $c_{max}(A) = 1/K$. For $E = \alpha_K H^\circ_{K+1}$ or $\alpha_K H_K$, the resulting sequences are ternary with $-\alpha_K$, 0, and $+\alpha_K$ as entries. The sequences are complex-valued when $E = \alpha_K F^\circ_{K+1}$.

For a given Δ, setting E equal to $\alpha_K F^\circ_{K+1}$ or $\alpha_K H^\circ_{K+1}$ yields one more sequence than setting E equal to $\alpha_K H_K$, since F°_{K+1} and H°_{K+1} are $(K + 1) \times K$ matrices, while H_K is a $K \times K$ matrix. The larger set can always be obtained since F_n exists for all n. However, for some applications it may be desirable to have ternary rather than complex sequences. This may not be possible with this method since Hadamard matrices H_n do not exist for n not a multiple of 4, with the exception of $n = 2$.

The first type of partial difference set is the planar (L,K) set with $L = K^2 - K + 1$, $K - 1$ a prime power.[3,4] For $K = 2$, we have $L = 3$ and $\Delta = \{0,1\}$. Letting $E = 2^{-\frac{1}{2}} F^\circ_3$ gives the three sequences

$$a^1 = 2^{-\frac{1}{2}}(1, 1, 0)$$
$$a^2 = 2^{-\frac{1}{2}}(\omega, \omega^2, 0)$$
$$a^3 = 2^{-\frac{1}{2}}(\omega^2, \omega, 0)$$

where ω is a cube root of 1 satisfying $\omega^2 + \omega + 1 = 0$. The autocorrelations and cross-correlations for the set of three sequences are

$$a^1 * a^1 = \frac{1}{2}(2, 1, 1)$$
$$a^2 * a^2 = \frac{1}{2}(2, \omega, \omega^2)$$
$$a^3 * a^3 = \frac{1}{2}(2, \omega^2, \omega)$$
$$a^1 * a^2 = \frac{1}{2}(-1, \omega^2, \omega)$$
$$a^1 * a^3 = \frac{1}{2}(-1, \omega, \omega^2)$$
$$a^2 * a^3 = \frac{1}{2}(-1, 1, 1).$$

Therefore, this set achieves the bound $W(3,3) = 1/2$. This set of sequences (for $K = 2$) is the smallest one guaranteed by the following.

THEOREM 1. *If $K - 1$ is a prime power, then there exists a set of $K + 1$ distinct complex-valued sequences of period $L = K^2 - K + 1$ with c_{max} equal to the bound $W(L,K+1) = 1/K$.*

The sequences of Theorem 1 are constructed from the planar difference sets for the prime power $K - 1$, and the truncated $(K + 1) \times K$ Fourier matrix $\alpha_K F^{\circ}_{K+1}$.

The second planar set occurs for $K = 3$, $L = 7$, and $\Delta = \{0,1,3\}$. We may let $E = 3^{-1/2}F^{\circ}_4$ or $3^{-1/2}H^{\circ}_4$, where

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

and

$$H^{\circ}_4 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix}.$$

For $E = 3^{-1/2}H^{\circ}_4$, the four sequences are

$$a^1 = 3^{-1/2}(1, 1, 0, 1, 0, 0, 0)$$

$$a^2 = 3^{-1/2}(1,-1, 0,-1, 0, 0, 0)$$

$$a^3 = 3^{-1/2}(-1, 1, 0,-1, 0, 0, 0)$$

$$a^4 = 3^{-1/2}(-1,-1, 0, 1, 0, 0, 0).$$

The bound $W(7,4) = 1/3$ is met by this set of ternary sequences.

11

The only known planar difference sets are those for $K - 1$ a prime power. Since 2 is the only prime power congruent to 2 modulo 4, the four sequences above form the only ternary set resulting from this construction which achieve the bound.

For $K - 1 = 3$, the set $\Delta = \{0,1,3,9\}$ is a planar difference set modulo 13. For this set, the matrix $\frac{1}{2} H_4$ can be used to construct four sequences

$$a^1 = \frac{1}{2}(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$$

$$a^2 = \frac{1}{2}(1, 1, 0,-1, 0, 0, 0, 0, 0,-1, 0, 0, 0)$$

$$a^3 = \frac{1}{2}(1,-1, 0, 1, 0, 0, 0, 0, 0,-1, 0, 0, 0)$$

$$a^4 = \frac{1}{2}(1,-1, 0,-1, 0, 0, 0, 0, 0, 1, 0, 0, 0).$$

The correlation coefficients (excluding the auto-correlation peaks) are all $-\frac{1}{4}$, 0, or $\frac{1}{4}$. The Welch bound for this case is $W(13,4) = (\frac{1}{17})^{\frac{1}{2}} = 0.243$. This set is the smallest of the type guaranteed by

THEOREM 2. *If $K - 1$ is a prime power congruent to 3 modulo 4, then there exists a set of K distinct ternary sequences of period $L = K^2 - K + 1$ which nearly achieve the bound. In particular $c_{max} = 1/K$, while $W(L,K) = (K^2 + 1)^{-\frac{1}{2}}$.*

The sets of Theorem 2 use $E = \alpha_K H_K$. The Hadamard matrix H_K for Theorem 2 may be constructed from the quadratic residues in the finite field GF(K-1).[3,4]

For the second type of partial difference set K may be any prime power, and $L = K^2 - 1$. These are special cases of the relative difference sets of Elliott and Butson.[5] A maximal linearly recurring sequence of degree 2 over the finite field GF(K) has period $L = K^2 - 1$. Every non-zero member of GF(K) occurs exactly K times in such a sequence, while 0 occurs $K - 1$ times. The set Δ of positions at which the 1's

occur form an (L,K) partial difference set. For K = 2 this set corresponds to the planar set in Z_3. For K = 3, the linearly recurring sequence associated with the primitive quadratic $x^2 + x + 2$ is (1,1,0,1,2,2,0,2). The resulting relative difference set is $\Delta = \{0,1,3\}$ in Z_8. The following two theorems result from the relative difference sets with K a prime power.

THEOREM 3. *If K is a prime power, then there exists a set of K + 1 distinct complex-valued sequences of period* $L = K^2 - 1$ *with* $c_{max} = 1/K$. *If* $K \equiv 3 \pmod 4$, *then a set of ternary sequences with the same parameters exists.*

THEOREM 4. *If K is a power of 2, then there exists a set of K distinct ternary sequences of period* $L = K^2 - 1$ *with* $c_{max} = 1/K$.

The ternary sequences of the second part of Theorem 3 are constructed using the quadratic residue Hadamard matrix over GF(K), that is, $E = \alpha_K H^{\circ}_{K+1}$. The Hadamard matrix H_K required in Theorem 4 can be constructed by the iterated tensor product

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_{2m} = H_2 \otimes H_m, \quad m = 2^r \geq 2, \quad r = 1,2,3\ldots .$$

The sets of Theorems 3 and 4 approach the bound W(L,K) as K and L increase. The bounds are

$$W(L,K+1) = (K/(K^3 + K^2 - K - 2))^{\frac{1}{2}} \quad \text{for Theorem 3,}$$

$$W(L,K) = ((K-1)/(K^3 - K - 1))^{\frac{1}{2}} \quad \text{for Theorem 4.}$$

Clearly each of these bounds approaches 1/K as K increases. Thus, the sets for Theorems 2, 3, and 4 are "asymptotically optimal."

4. THE BINARY SEQUENCES

In this section we construct sets of sequences of period $L = 2^{2m} - 1$ from linear cyclic error-correcting codes over GF(2) of length L. For γ an element of $GF(2^n)$ let $u(\gamma)$ denote a linearly recurring sequence associated with the minimal polynomial of γ over GF(2). The period $\pi(\gamma)$ of $u(\gamma)$ is the multiplicative order of γ in $GF(2^n)$, and must divide $2^n - 1$. Let $v(\gamma)$ be the $(2^n - 1)$-dimensional vector over GF(2) formed by juxtaposing $I(\gamma)$ periods of the sequence $u(\gamma)$, where $I(\gamma) = (2^n - 1)/\pi(\gamma)$. If γ is a primitive element of $GF(2^n)$, then $I(\gamma) = 1$, and $v(\gamma)$ together with all of its cyclic shifts generate an n-dimensional cyclic code over GF(2) with minimum weight 2^{n-1}. Now suppose $\delta = \gamma^r$, and let C(r) be the code generated by all cyclic shifts of both $v(\gamma)$ and $v(\delta)$. C(r) is a cyclic (n+d)-dimensional code, if δ is not conjugate to γ, where d is the degree of δ over GF(2). Kasami, Lin, and Peterson have computed the weight distributions of several such codes.[6] C(r) decomposes into classes of cyclically equivalent vectors. By selecting one representative from each class of period $2^n - 1$ and replacing each 0 and each 1 with $-(2^n - 1)^{-\frac{1}{2}}$ and $+(2^n - 1)^{-\frac{1}{2}}$, respectively, a set A(r) of normalized binary sequences is obtained. The Gold sequences result from letting

$$r = \left.\begin{array}{ll} 2^{(n+1)/2} + 1 & \text{for } n \text{ odd} \\ 2^{(n+2)/2} + 1 & \text{for } n \text{ even} \end{array}\right\}.$$

In this case C(r) has dimension 2n, and the $2^{2n} - 1$ non-zero code words fall into $2^n + 1$ classes, each of period $2^n - 1$, provided r is relatively prime to $2^n - 1$. (When g.c.d. $(r, 2^n - 1) = s > 1$, C(r) contains only 2^n classes of period $2^n - 1$. The remaining $2^n - 1$ non-zero code words have period $(2^n - 1)/s$.) The family A(r) contains $M = 2^n + 1$ sequences of period $L = 2^n - 1$, with $c_{max} = r/L$ (see footnote 2). Thus, for the Gold sequences c_{max} is approximately $2L^{-\frac{1}{2}}$, $2^{\frac{1}{2}}L^{-\frac{1}{2}}$ for n even, odd, respectively; whereas $W(L,M) = W(2^n - 1, 2^n + 1)$ is approximately $L^{-\frac{1}{2}}$.

For our sequences we let $n = 2m$ and $r = 2^m + 1$. The resulting code $C(r)$ has length $L = 2^{2m} - 1$, dimension $3m$ and minimum weight $2^{m-1}(2^m - 1)$. In fact the only non-zero weights occurring in $C(r)$ are $2^{m-1}(2^m - 1)$, 2^{2m-1}, and $2^{m-1}(2^m + 1)$, see footnote 6. Thus, the cross-correlation coefficients and auto-correlation side-lobes for the set $A(r)$ of sequences of period L assume only the three values $(-2^m - 1)/L$, $-1/L$, and $(2^m - 1)/L$. It follows that $c_{max} = (2^m + 1)/L = 1/(2^m - 1)$. This approximates c_{max} for Gold sequences of period $2^{2m+1} - 1 = 2L + 1$. The $3m$-dimensional code $C(r)$ contains a single class of vectors of period $2^m - 1$ generated by δ. The remaining $2^{3m} - 2^m$ vectors fall into 2^m classes of period $L = 2^{2m} - 1$. Thus, $M = 2^m$ and the bound is $W(L,M) = ((2^m - 1)/(2^{3m} - 2^m - 1))^{\frac{1}{2}}$, which is approximately equal to $L^{-\frac{1}{2}}$.

The first example of this construction is for $m = 2$, $L = 15$, $M = 4$. Letting γ be a root of $x^4 + x + 1$, and $\delta = \gamma^5$, we have

$$v(\gamma) = (0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1),$$

$$v(\delta) = (0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1).$$

The four cyclically distinct vectors in $C(r)$ are $v(\gamma)$ together with $v(\gamma)$ added to each of the three shifts of $v(\delta)$. For the associated set $A(r)$ we have $L = 15$, $M = 4$, and $c_{max} = 1/3$; while $W(15,4) = (3/59)^{\frac{1}{2}} = 0.225$.

INITIAL DISTRIBUTION

8 Naval Sea Systems Command
- NSEA-0333 (2)
- NSEA-0341 (1)
- NSEA-036 (1)
- NSEA-654312A (1)
- Technical Library (2)
- PMS-404-52 (1)

4 Naval Air Systems Command
- AIR-350 (1)
- AIR-360D (1)
- AIR-370 (1)
- AIR-5324 (1)

1 Chief of Naval Material (MAT-032B)
1 Naval Surface Weapons Center, White Oak Laboratory (R. Eby)
1 Naval Surface Weapons Center, Dahlgren Laboratory (J. Lynch)
1 Army Materiel Systems Analysis Agency (J. Kramar)
1 Harry Diamond Laboratories (S. Peperone)
1 Air Force Armament Laboratory, Eglin Air Force Base (DLJF)
1 Applied Physics Laboratory, JHU, Silver Spring, Md. (B. Dobbins)
1 Institute for Defense Analyses, Arlington, Va. (Dr. F. S. Atchison)
1 Naval Research Laboratory (Technical Library)
1 Naval Electronics Laboratory, San Diego (Technical Library)
1 Naval Undersea Center, San Diego (Technical Library)
1 Naval Postgraduate School, Monterey (Technical Library)
2 Office of Naval Research
- ONR-432 (1)
- ONR-437 (1)

1 Office of Naval Research Branch Office, Pasadena (R. Lau)

16